AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Massachusetts

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

ONE KYOCERA CELLULAR TELEPHONE, IN THE CUSTODY OF ATF

Case No. 15-mj-6008-MPK

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Affidavit, Attachments A and B.

located in the possession of ATF District of Massachusetts, there is now concealed *(identify the person or describe the property to be seized)*:

See Affidavit of Mattheu P. Kelsch, Special Agent, ATFattached.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC Section 371; 18 USC Section 922(a)(6); 922 (g)(1)	Conspiracy to make a False Statement during the Acquisition of a Firearm; Felon in Possession of a Firearm and Ammunition.

The application is based on these facts:

See supporting Affidavit.

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Mattheu P. Kelsch, Special Agent, ATF
Printed name and title

Sworn to before me and signed in my presence.

Date: 03/18/2015

Judge's signature

City and state: Boston, MA

M. Page Kelley, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

IN RE: ORDER REQUIRING GOOGLE, INC. TO ASSIST IN THE EXECUTION OF A SEARCH WARRANT ISSUED BY THIS COURT	Magistrate No. 15-MJ-6008-MPK **Filed Under Seal**

APPLICATION

I. INTRODUCTION

The United States of America, by and through Carmen M. Ortiz, United States Attorney, and Glenn A. MacKinlay, Assistant United States Attorney, hereby moves this Court under the All Writs Act, 28 U.S.C. § 1651, for an order requiring Google, Inc. ("Google") to assist in the execution of a federal search warrant by bypassing the lock screen of an Android device, specifically, an Android device.

II. FACTS

The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) currently has in its possession an Android device that is the subject of a search warrant issued by this Court. Initial inspection of the Android device reveals that it is locked. Because the Android device is locked, law enforcement agents are not able to examine the data stored on the Android device as commanded by the search warrant.

The Android device is a Kyocera. It has Model C5170, FCC ID: V65C5170, DEC: 268435459916695431, HEX: A0000027FECO87 on the Sprint PCS network with access number (phone number) 617-386-0286 (the "Android Device").

Google, the creator of the Android operating system and producer of the Android device, may have the capability of bypassing the Android device's lock and thereby retrieving data

stored on the Android device that is not currently accessible to ATF. This Application seeks an order requiring Google to use any such capability, so as to assist agents in complying with the search warrant.

The United States requests that the Court order that Google, if necessary, must reactivate the Google account associated with the Android Device for the limited purpose of complying with the search warrant.

Further, the United States requests that Google be directed to: (1) provide a single password reset for the Android device; (2) provide the new password to the law enforcement officer executing the search warrant; and (3) upon unlocking the target Android device, again reset the Google account password promptly upon notice that the imaging of the phone is complete, without providing it to the law enforcement officer or agency so as to prevent future access.

Further, the United States represents that the reset process may not be unobtrusive to the subject and that the subject may receive notice to one or more accounts of the reset. Accordingly, the United States requests that the Court order that any such notice is not a violation of any seal or nondisclosure requirement.

Finally, the United States does not seek authority to use the new password to attempt to access the subject's online accounts other than as synchronized on, and stored in, memory within the target device at the time of execution of the warrant, and does not object to the Court prohibiting such use of the password to be provided by Google.

III. DISCUSSION

The All Writs Act provides that "[t]he Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a). As the Supreme Court explained, "[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute." Pennsylvania Bureau of Correction v. United States Marshals Service, 474 U.S. 34, 43 (1985). "The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice... and encompasses even those who have not taken any affirmative action to hinder justice." United States v. New York Tel. Co., 434 U.S. 159, 174 (1977). Specifically, in United States v. New York Tel. Co., the Supreme Court held that the All Writs Act permitted district courts to order a telephone company to effectuate a search warrant by installing a pen register. Under the reasoning of New York Tel. Co., this Court has the authority to order Google to use any capabilities it may have to assist in effectuating the search warrant for the Android device by unlocking the Android Device.

The government is aware, and can represent, that in other cases, courts have ordered Google to assist in effectuating a search warrant by unlocking other Android devices under the authority of the All Writs Act. Additionally, Google has complied with such orders.

The requested order would enable agents to comply with this Court's warrant commanding that the Android device be examined for evidence identified by the warrant. Examining the Android device without Google's assistance, if it is possible at all, would require

significant resources and may harm the Android device. Moreover, the order is not likely to place any unreasonable burden on Google.

Respectfully submitted,

Glenn A. MacKinlay
Assistant U.S. Attorney

Date: March 18, 2015

IN THE UNITED STATES DISTRICT COURT
FOR DISTRICT OF MASSACHUSETTS

IN THE MATTER OF THE SEARCH OF KYOCERA CELLULAR TELEPHONE, MODEL: C5170, FCC ID: V65C5170, DEC: 268435459916695431, HEX: A0000027FECO87, CURRENTLY LOCATED AT 10 CAUSEWAY STREET, ROOM 701, BOSTON, MA 02222	Case No. 15-MJ-6008-MPK

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

I, Mattheu P. Kelsch, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—one electronic device, which is currently in law enforcement possession, and the extraction from this device of electronically stored information described in Attachment B.

2. I am employed as a Special Agent (S/A) with the United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), and have been so employed for approximately 14 years. During that time, I successfully completed Criminal Investigator School and New Professional Training at the Federal Law Enforcement Training Center in Glynco, Georgia, and the Bureau of Alcohol, Tobacco and Firearms Interstate Nexus School in Martinsburg, West Virginia. Prior to that, I was employed as an officer for the legacy agency, the Immigration and Naturalization Service.

3. As an ATF Special Agent, I assist in conducting investigations into the unlawful possession of firearms. Through training, investigations and experience, I have taken part in cases relating to the trafficking of firearms, the use and possession of firearms by persons prohibited by law and the possession of illegal firearms. I am familiar and have participated in various methods of investigations, including, but not limited to: electronic surveillance, physical surveillance, interviewing and general questioning of witnesses, use of confidential informants, use of cooperating witnesses, use of toll records and subscribers information. I have also debriefed confidential informants and cooperating witnesses regarding the habits and practices of people engaged in the illegal trafficking of firearms. Furthermore, I have conducted and participated in numerous investigations to include: crime scene investigations, collection of evidence, interviews and the execution of search warrants.

4. Through my training, experience and interaction with experienced S/As, Task Force Officers (TFOs) and other investigators, I have become familiar with the methods employed by armed criminals and criminal organizations in particular, in their efforts to communicate with each other and to plot and conspire to commit violent crimes.

5. I know that people who commit and conspire such crimes in concert with other individuals commonly maintain records that reflect names, addresses and/or telephone numbers of their associates in their telephones; they also maintain records of communications such as telephone call logs, chats and text messages; in addition they take photographs of themselves or induce others to photograph them, their associates, their property, and their product. These individuals usually maintain these records of communication and photographs in their possession and in cellular phones.

6. This affidavit is based upon my experience and training as a Special Agent of the ATF, my personal participation in the investigation, my review of ATF records, my review of reports prepared and maintained by local and state agencies, and information provided to me by other law enforcement officials. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

7. The property to be searched is:

Kyocera, Model: C5170, FCC ID: V65C5170, DEC: 268435459916695431, HEX: A0000027FEC087;

seized from an orange Mustang, driven by Shayne PARKER on April 14, 2014, currently being held as evidence by the ATF at 10 Causeway Street, Room 701, Boston, MA 02222 ("the Device").

8. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

9. On or about March 23, 2014, ATF Special Agent Coughlin received a telephone call from Trooper Charles Newton of the New Hampshire State Police. Trooper Newton advised S/A Coughlin that while he was on a day off he entered the Alstead Gun Shop in Alstead, NH, a federally licensed firearms dealer, and observed two black males, subsequently identified as Ronald SCOTT and Shayne PARKER, and a white male subsequently referred to as "CW," inside the firearms store. According to Trooper Newton, the men had a strong odor of marijuana

on their clothing. While inside the store, Trooper Newton took a photograph of the white male with his cell phone. Trooper Newton said the men left the store when he (unsuccessfully) attempted to engage them in conversation. After the men left the store, Trooper Newton spoke with the clerk. According to the clerk, on approximately March 8th or 9th, 2014, the two black males were in the store looking at three firearms. On March 10, 2014, a female, subsequently identified as Sandra Egbert, purchased the three firearms which the two men were looking at a few days earlier.

10. On March 23, 2014, CW was arrested by Keene Police Department for possession of a narcotic drug, operating under the influence of drugs/liquor and hunting while operating a vehicle. When CW was arrested, Keene Police Department seized a .410 bolt action shotgun. According to CW, Shayne PARKER sold him the shotgun.

11. Trooper Newton viewed CW's arrest photograph and recognized it to be the white male that was in the Alstead Gun Shop earlier that same day with the two black males. CW later agreed to cooperate with law enforcement as outlined below.

12. On April 3, 2014, Trooper Newton telephoned S/A Coughlin and told him that the Alstead Gun Shop reported to him that Egbert had just purchased an additional 5 firearms. S/A Coughlin reviewed a Report of Multiple Sale for that transaction and learned that on April 3, 2014, Egbert acquired the following firearms:

- Chiappa, Model 1911-22, .22 caliber pistol, serial number 13G05427;
- IOI Inc., Model Hell Cat, .380 pistol, serial number X0330;
- Taurus, Model PT738, .380 pistol, serial number 34028D;
- Bersa, Model 383-A, .380 pistol, serial number 184613; and

- Iver Johnson, Model safety auto, .32 caliber revolver, serial number C49293.

13. On April 3, 2014, members of the ATF and the New Hampshire State Police interviewed CW at a residence in New Hampshire. The CW stated that it had facilitated the "straw" purchases of approximately twenty firearms using Egbert and a second female, Melanie LaMott.[1] The CW explained that it owed a drug debt to an individual it knew as "Jay." On April 4, 2014, the CW was shown two separate photo arrays by Trooper Newton. CW identified the photograph of Ronald SCOTT as the individual known to him as "Jay."

14. According to CW, SCOTT suggested that CW purchase firearms for him to pay off CW's drug debt. CW agreed to facilitate the purchase of firearms for SCOTT to pay down his drug debt. SCOTT provided CW with money to purchase the firearms.

15. CW stated that each purchase occurred in the much the same manner. SCOTT telephoned or sent a text message to CW from telephone number 857-234-3498 advising CW that he wanted CW to purchase firearms. CW admitted that he arranged at least four separate purchases of firearms using two women, Sandra Egbert and Melanie LaMott. S/A John Forte examined CW's cell phone, with CW's consent, and observed a text message from "Jay" (SCOTT) received on March 29, 2014 at 10:40 a.m. which stated, "On the way now meet us in Hudson." S/A Forte also observed several text messages to CW from telephone number 857-

---

[1] A subsequent investigation revealed that CW also used a third individual, Richard Burke, to straw purchase firearms. During an interview with Burke, CW's sister texted Burke stating CW "says that if ATF calls to just tell them he sold the guns to him for money and he sold them for money but ge don't know who and to erase this message." Burke admitted that he purchased firearms for CW. SA Coughlin confronted CW about Burke and CW admitted that it used Burke to straw purchase firearms as well. CW also denied telling anyone that it was working with ATF but after being confronted with the text message to Burke, CW admitted that it did tell someone about its cooperation with ATF.

234-3498 on April 1, 2014, April 2, 2014 and April 3, 2014 trying to arrange a meeting. Lastly, S/A Forte also observed a text message dated April 3, 2014 from telephone number 347-994-6804 which stated, "Its Jay answer the phone." (On March 29, 2014, Melanie Lamott attempted to purchase a firearm at Pete's Gun & Tackle in Hudson, NH but was delayed. On April 3, 2014, Sandra Egbert successfully purchased 5 firearms from Alstead Gun Shop.)

16. Once the females purchased the firearms, they gave the firearms to CW who subsequently met with SCOTT and gave SCOTT the firearms. Each time CW met with SCOTT, he was in a vehicle driven by a person CW knew as "Riot." On April 4, 2014, the CW was shown a photo array by Trooper Newton. and identified the photograph of Shayne PARKER as the individual known to him as "Riot."

17. Prior to meeting with SCOTT, PARKER, using telephone number 617-386-0286, telephoned CW to obtain GPS coordinates for the meet location. In addition, the investigation revealed that PARKER used telephone number 617 386 0286 to telephone CW on at least 2 occasions including a 51 second phone call to CW on April 2, 2014 (one day before Egbert acquired five handguns from the Alstead Gun Shop on April 3, 2014).

18. On April 8, 2014, the CW using telephone number 603-757-3563 placed a recorded telephone call and texted SCOTT at telephone number 857-234-3563 while in the presence of S/A's Coughlin and Forte. During the contact with the CW, SCOTT sent a text message which read, "You know got 1500 and 7g." The CW understood the text message to mean that SCOTT had $1500.00 and 7 grams of crack cocaine for the purchase of firearms. At the request of law enforcement, the CW stalled the potential transaction. In a second recorded conversation with the CW, SCOTT agreed to provide 5 grams of "white" (which the CW

understood to be cocaine) and four grams of "brown" (which the CW understood to be heroin) in exchange for three, nine millimeter handguns. SCOTT agreed to pay CW $100.00 for setting up the deal. SCOTT told CW to set up the deal, call him and he would go to New Hampshire since he really needed the guns.

19. On or about April 9, 2014, S/A Kelsch applied for and received a court order for "a Pen Register and Trap and Trace with Caller Identification Device and Cell Site Location Authority" for the phones of Ronald SCOTT (857) 234-3498 (T-Mobile) and Shayne PARKER (617) 386-0286 (SPRINT PCS). In essence, the providers or carriers of the listed phones sent out signals every 15 minutes and obtained GPS co-ordinates with respect to the location of the devices. These GPS locations (where the phones were "pinged") were then transmitted to S/A Kelsch via email. S/A Kelsch set up an auto forward for emails related to "pinging" these 2 particular cell phones and selected S/A John Forte (Manchester, NH ATF) as a recipient of the GPS co-ordinate information.

20. On April 14, 2014, SCOTT called CW from telephone number (857) 234-3498 several times in order to meet with CW for the purported deal. In a conversation monitored by S/A Coughlin, SCOTT gave his phone to an individual who identified himself as "Riot" to get directions to the meeting site from CW.

21. On April 14, 2014, CW telephoned SCOTT at (857) 234-3498 and instructed SCOTT and PARKER to meet him at the Home Depot parking lot in Keene, New Hampshire to conduct the deal.

22. On April 14, 2014, S/A Forte received GPS co-ordinate information via email from both cell phone carriers and the 2 phones were "pinging" North of Boston. Later in the afternoon, S/A Forte advised S/A Coughlin that both cell phones were pinging in Amherst, NH. After several monitored telephone conversations between CW and SCOTT, the cell phones started "pinging" in Dublin, NH (which is on the way to Keene via Route 101).

23. Later that day, SCOTT and PARKER entered the Home Depot parking lot and PARKER parked his vehicle next to CW's vehicle in the parking lot as instructed by CW. Based upon the information provided to S/A Coughlin by S/A Forte on April 14, 2014, S/A Coughlin had reason to believe that at least 2 communication devices belonging to SCOTT and PARKER would be located within the SCOTT/PARKER vehicle.

24. SCOTT and PARKER were subsequently arrested by ATF. Law enforcement seized approximately 14 grams of a white substance, which field tested positive for crack cocaine, from SCOTT which was stashed underneath his scrotum. The crack cocaine was packaged in two baggies. One baggie contained 18 individual baggies containing crack cocaine and the second baggie contained 6 individual baggies containing crack cocaine. Trooper Charles Newton applied for and received authority to execute a state search warrant for PARKER's vehicle. On April 14, 2014, Trooper Newton searched PARKER's vehicle and among other items, Trooper Newton seized the following, subsequently referred to as the "Devices:"

a. Kyocera, Model: C5170, FCC ID: V65C5170, DEC: 268435459916695431, HEX: A0000027FECO87 OR A0000027FEC087 (UNKNOWN IF 11TH CHARACTER IS AN "O" OR A "0")

b. Samsung, Mini Tablet, GALAXY NOTE 3, Model: SM-N900T, FCC ID: A3LSMN900T, IMEI: 357518/05/440924/8, Serial Number: RV8DC093NVM; and

c. TomTom START, Model: 4EFOO, Serial Number/C_NO: GU4292B01993, (4EF0.017.00).

25. The above devices are currently in the lawful possession of the ATF. The NHSP obtained the Devices from PARKER's vehicle at the time of SCOTT and PARKER's arrest. Other agents and S/A Coughlin have only powered on the Devices to attempt to confirm its telephone number (unsuccessfully) and have not conducted any other search of the Devices.

26. The Devices are currently in storage at the ATF facility located at 10 Causeway Street, Room 701, Boston, MA 02222. In my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the ATF.

27. On May 9, 2014, a search and seizure warrant was issued for the Devices in the United States District Court for the District of New Hampshire. Pursuant to that warrant, on May 12, 2014, S/A Kelsch powered on the Kyocera, model C5170 device to attempt a forensic examination and found it to be locked using a pin type lock code. The device is unable to be unlocked using current readily available forensic methods. No further search was conducted and the search warrant was returned to the United States District Court for the District of New Hampshire. I now seek a search warrant in the District of Massachusetts to search the Device and also am requesting an order compelling Google, Inc., the service provider for the Device, to provide the password that will permit the proper execution of this search warrant.

28. Subsequent investigation revealed that there were previous firearms transactions involving the CW, SCOTT, PARKER and Lamott. One such purchase occurred on or about March 22, 2014. Lamott under the direction of the CW, traveled to the Sporting and Hunting Depot, located in Charlestown, NH and purchased four firearms. Lamott and the CW, driving in the CW's vehicle, later met with SCOTT and PARKER. SCOTT and PARKER were operating the orange Mustang, registered to PARKER and described earlier in this affidavit. Lamott and the CW were instructed to follow SCOTT and PARKER to Boston, MA. While en-route, the parties stopped at a Dick's Sporting Goods located in Keane, NH. SCOTT and Lamott entered the store and purchased five boxes of ammunition. One of those boxes of ammunition was described as .380 caliber manufactured by CCI. The CW, Lamott, SCOTT and PARKER then proceeded to 233 River Street, Unit 104, Boston, MA where those parties and others handled the firearms and ammunition in the bedroom area.

29. On April 14, 2014, a Federal Search Warrant was executed at 233 River Street, Unit 104, Boston, MA. Among the items seized were a Ruger firearm, a box of .380 ammunition manufactured by CCI and a portion of the receipt from Dick's Sporting Goods from the March 22, 2014 transaction. The SKU # on the CCI .380 caliber ammunition box recovered during the search matched that of one of the boxes of ammunition purchased at the Dick's Sporting Goods store.

30. Subsequent laboratory testing conducted by the Boston Police Latent Print Unit, revealed a fingerprint matching that of the right index finger of PARKER on the inner tray of the CCI .380 ammunition package.

TECHNICAL TERMS

31. Based on my training and experience, as well as my conversations with other law enforcement officers who have experience working with electronic devices, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

32. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

33. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of their use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

34. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

35. *Manner of execution.* Because this warrant seeks only permission to examine the Device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

36. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

I declare that the foregoing is true and correct.

Mattheu P. Kelsch
Special Agent
Bureau of Alcohol, Tobacco, Firearms, and Explosives

Subscribed and sworn to before me this 18th day of March, 2015:

PAGE M. KELLEY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is a Kyocera cellular phone, Model: C5170, FCC ID: V65C5170, DEC 268435459916695431, seized on April 14, 2014, currently being held as evidence by the ATF at 10 Causeway Street, Room 701, Boston, MA 02222.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. §371, §922(a)(6), and §922(g)(1), and involve Ronald SCOTT; Mitchell RIDDELL; Shayne PARKER; Sandra EGBERT; Melanie LAMOTT; Rory RIDDELL and Richard BURKE, including:

   a. Records or other information related to the acquisition or possession of firearms from March 1, 2014, to the present;

   b. all stored electronic and wire communications and information in memory within the mobile device, including email, instant messaging, or other communications, and including any content that may be synchronized to or on the device from any service or application utilized by the subject as of the date of execution of the search warrant (i.e., the date of the password reset);

   c. Records or other information related to the acquisition of controlled substances, including cocaine base (crack cocaine) and heroin, including, types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions from March 1, 2014 to the present;

   d. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information) from March 1, 2014 to the present;

   e. any information recording the schedule or travel of Ronald SCOTT; Mitchell RIDDELL; Shayne PARKER; Sandra EGBERT; Melanie LAMOTT; Rory RIDDELL; and Richard BURKE from March 1, 2014, to the present;

   f. records reflecting any contacts or communications between or among Ronald SCOTT; Mitchell RIDDELL; Shayne PARKER; Sandra EGBERT; Melanie LAMOTT; Rory RIDDELL; and Richard BURKE;

   g. all text messages between or among Ronald SCOTT; Mitchell RIDDELL; Shayne PARKER; Sandra EGBERT; Melanie LAMOTT; Rory RIDDELL; and Richard BURKE; and

   h. GPS historical data.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the Internet Protocol addresses to communicate over the Internet, including:

a. records of Internet Protocol addresses used; and

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

4. If necessary, and if the device can establish a data connection to the mobile network of the underlying service provider by law enforcement, Google is ordered to reactivate the Google account associated with the mobile device for the limited purpose of complying with the search warrant. Before beginning the unlock procedure, Google shall coordinate the time of executing the unlock procedure with the law enforcement officer executing the search warrant (hereafter "the law enforcement officer") to ensure all parties are prepared to conduct the device unlock.

5. Google is directed to provide a single password reset for the mobile device, to provide the new password to the law enforcement officer, and upon unlocking the target mobile

device, again reset the Google account password promptly upon notice from the law enforcement officer that the unlocking of the phone is complete. without providing it to the law enforcement officer or agency so as to prevent future access. The reset process need not be unobtrusive to the subject and the subject may receive notice to one or more accounts of the reset as a part of this unlock process; such notice is not a violation of any seal or nondisclosure requirement.